Amendments to the Claims:

This listing of claims will replace all prior versions, and l iš ings, of claims in the application:

Listing of Claims:

1. (Currently Amended) A data processing device, comprising in particular an electronic memory component, comprising a plurality of access-secured sub-areas, in particular a plurality of access-secured memory areas, each having at least one assigned parameter, in particular address, the device configured such that characterized in that the parameter of at least one sub-area is may be encrypted only in certain areas, i. e. in dependence depending on at least one further sub-area.

2. (Currently Amended) The A data processing device as claimed in claim 1, wherein characterized in that the encrypted parameter to be encrypted may be is encrypted as a function of in dependence, in particular as function, on at least one parameter of the further sub-area.

3. (Currently Amended) The A data processing device as claimed in claim 2, wherein at least one of characterized in that

        [[- the]] an input value to the function and/or

        [[- the]] a return value from the function

is more than one bit wide.

4. (Currently Amended) The A data processing device as claimed in claim 1, wherein characterized in that the memory component comprises takes the form of

        [[-]]an erasable programmable read only memory,E[rasable]P[rogrammable]R[ead]O[nly]M[emory],

        [[-]]an electrically erasable programmable read only memory E[lectrically]E[rasable]P[rogrammable]R[ead]O[nly]M[emory] or

[[-]]a [[F]]flash memory.

5. (Canceled)

6. (Currently Amended) A method of securing access to an electronic memory, comprising:

_____ encrypting at least one parameter, ~~in particular the address,~~ of at least one of a plurality of access-secured sub-areas of the electronic memory, ~~sub-area, in particular at least one access-secured memory area, of at least one data processing device, in particular at least one electronic memory component characterized in that~~ wherein the parameter to be encrypted of the sub-area is encrypted only in certain areas, ~~i. e. in dependence on at least one further sub-area~~ to increase security of the electronic memory.

7. (Currently Amended) The ~~A~~ method as claimed in claim 6, wherein ~~characterized in that~~ the parameter to be encrypted of the sub-area is encrypted ~~in dependence, in particular~~ as a function, ~~on~~ of at least one parameter of a ~~the~~ further sub-area.

8. (Currently Amended) The ~~A~~ method as claimed in claim 7, c aracterized in that the function f,(a) is one-to-one.

9. (Currently Amended) The ~~A~~ method as claimed in claim 6, wherein ~~characterized in that~~ the access-secured sub-areas, ~~in particular the access-secured memory areas,~~ are secured separately.

10. (Currently Amended) A ~~Use of at least one~~ data processing device, ~~in particular at least one electronic memory component, as claimed in claim 1 in at least one chip unit, in particular~~ comprising an electronic memory component, comprising a plurality of access-secured memory areas, each having at least one assigned parameter, the device configured such that the

parameter of at least one sub-area is encrypted only in certain areas depending on at least one further sub-area, the data processing device utilized in at least one of

[[- in at least]] a one smart card controller,

[[- in at least one]] a reader I̶[integrated]̶ ̶C̶[circuit]̶, or

[[- in at least one]] a cryptography chipset,

for application example in at least one the field of audio and/or video encryption.

11. (New) The data processing device as claimed in claim 1, wherein the at least one assigned parameter comprises an address.

12. (New) The method as claimed in claim 6, wherein the at least one parameter comprises an address.